Claims

1. (Currently amended) In a distributed computing environment, a method for managing an electronic record for compliance with ~~a~~ pre-determined network security rules ~~policy~~ of an organization, the method comprising:

creating an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the pre-determined network security rules ~~policy~~;

storing the at least one electronic tag in a central repository;

sending the electronic record from the distributed computing environment to a recipient; and

automatically denying a request to delete the electronic record before expiration of the deletion prevention ~~specified~~ time period associated with the electronic tag.

2. (Previously presented) The method of claim 1, further comprising deleting the electronic record and selectively deleting the at least one electronic tag.

3. (Previously presented) The method of claim 1, further comprising storing the electronic record.

4. (Currently amended) The method of claim 1, further comprising determining whether the request is consistent with the network security rules ~~policy~~.

5. (Currently amended) The method of claim 1, wherein: the distributed computing environment comprises a computer having a registry and a user profile, and

wherein creating the electronic tag comprises generating a reference code and creating, ~~wherein~~ the electronic tag ~~is generated~~ at least in part as a function of at least one of the registry, the user profile, and the reference code.

6. (Previously presented) The method of claim 5, wherein generating the reference code comprises reading the electronic record.

7. (Previously presented) The method of claim 5, wherein the reference code comprises a classification code and an index code.

8. (Previously presented) The method of claim 7, wherein the classification code is selected from a group comprising business email, personal email, intramail, bulletin board, minutemail, and purgemail.

9. (Previously presented) The method of claim 7, wherein the index code identifies the contents of the electronic record and the recipient of the electronic record.

10. (Previously presented) The method of claim 1, wherein creating the electronic tag comprises:

reading a stored electronic tag; and

generating an electronic tag in response to accessing an electronic record.

11. (Previously presented) The method of claim 1, wherein the electronic record comprises an email message.

12. (Previously presented) The method of claim 1, wherein sending the electronic record comprises:

reading the electronic tag; and

generating a new electronic tag at least in part as a function of the read electronic tag, a computer registry, a user profile, and a reference code.

13. (Currently amended) In a distributed computing environment, an apparatus for managing an electronic record for compliance with ~~a~~ network security rules ~~policy~~, the apparatus comprising:

a computer system comprising at least one processor and at least one memory, the computer system being adapted and arranged to

create an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the network security rules ~~policy~~;

store the at least one electronic tag in a central repository;

send the electronic record from the distributed computing environment to a recipient; and

automatically deny a request to delete the electronic record before expiration of the deletion prevention ~~specified~~ time period associated with the electronic tag.

14. (Previously presented) The apparatus of claim 13, wherein the computer system is further adapted and arranged for purging the electronic record by deleting the electronic record and selectively deleting the at least one electronic tag.

15. (Currently amended) The apparatus of claim 13, wherein the computer system is further adapted and arranged for selectively determining whether the request is consistent with the network security rules ~~policy~~.

16. (Previously presented) The apparatus of claim 13, wherein the distributed computing environment comprises a computer having a registry and a user profile, wherein the computer system is configured and arranged to:

generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

17. (Currently amended) In a distributed computing environment, an article of manufacture for managing an electronic record for compliance with ~~a~~ network security rules ~~policy~~, the article of manufacture compromising a computer-readable storage medium having a computer program embodied therein that causes the distributed computing environment ~~computer network~~ to:

create an electronic tag that identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the network security rules ~~policy~~;

store the electronic tag in a central repository;

send the electronic record from the distributed computing environment to a recipient; and

automatically deny a request to delete the electronic record before expiration of the deletion prevention ~~specified~~ time period associated with the electronic tag.

18. (Currently amended) The article of claim 17, wherein the computer program further causes the distributed computing environment ~~computer network~~ to purge the electronic record by deleting the electronic record and selectively deleting the at least one electronic tag.

19. (Currently amended) The article of claim 17, wherein the computer program further causes the distributed computing environment ~~computer network~~ to store the electronic record.

20. (Currently amended) The article of claim 17, wherein the computer program further causes the distributed computing environment ~~computer network~~ to selectively determine whether the request is consistent with the network security rules ~~policy~~.

21. (Currently amended) The article of claim 17, wherein the distributed computing environment comprises a computer having a registry and a user profile, wherein the computer program further causes the distributed computing environment ~~computer network~~ to generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

22. (Currently amended) The article of claim 17, wherein the computer program further causes the distributed computing environment ~~computer network~~ to:

read a stored electronic tag; and

generate a further electronic tag in response to accessing an electronic record.

23. (Currently amended) In a distributed computing environment, a method for managing an electronic record for compliance with ~~a~~ pre-determined network security rules ~~policy~~ of an organization, the method comprising:

creating an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the pre-determined network security rules ~~policy~~;

storing the at least one electronic tag in a central repository;

sending the electronic record to a recipient;

automatically denying a request to delete the electronic record before expiration of the deletion prevention ~~specified~~ time period associated with the electronic tag; and

automatically monitoring compliance with the network security rules ~~policy~~ as a function of the electronic tag.

24. (New) The method of claim 1, further comprising overriding the denial of the request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag when the request is received from a user having a security privilege to override the denial.

25. (New) The apparatus of claim 13, wherein the computer system is further adapted and arranged for overriding the denial of the request to delete the electronic record before expiration of the deletion prevention time period associated with the

electronic tag when the request is received from a user having a security privilege to override the denial.

26. (New) The article of claim 17, wherein the computer program further causes the distributed computing environment to override the denial of the request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag when the request is received from a user having a security privilege to override the denial.